

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-091744

(43)Date of publication of application : 29.03.2002

(51)Int.Cl.

G06F 3/12
 B41J 5/30
 B41J 29/00
 G06K 17/00
 G09C 1/00
 H04L 9/08

(21)Application number : 2000-285294

(71)Applicant : CANON INC

(22)Date of filing : 20.09.2000

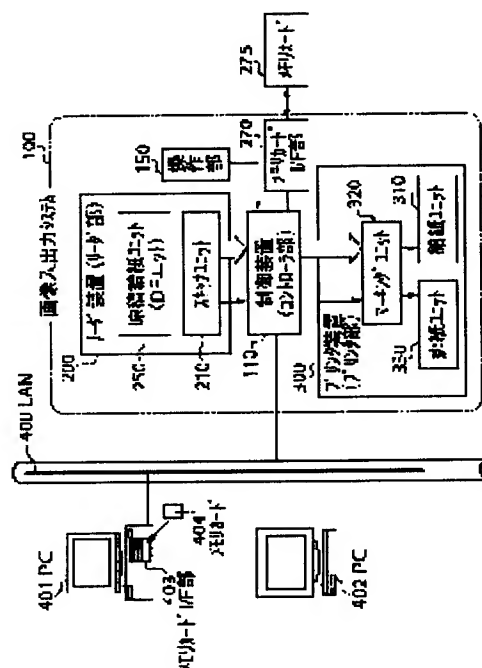
(72)Inventor : KASAI KAZUHIRO
TAKARAGI YOICHI

(54) IMAGE INPUT DEVICE, IMAGE OUTPUT DEVICE, IMAGE INPUT/ OUTPUT DEVICE, IMAGE DATA ENCIPHERING METHOD, IMAGE DATA DECIPHERING METHOD AND STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an image input device, an image output device, an image input/output device, an image data preserving method, an image data output method and a storage medium by which the reliability of data can be improved by preventing image file data in a memory card from being fraudulently altered or unauthorizedly utilized by a third person.

SOLUTION: When preserving the image file data on a memory card 275, a controller 110 preserves the images file data on the memory card 275 after enciphering them while using the public key of a public key cipher system and when outputting the image file data, which are enciphered by using the public key of the public key cipher system, on the memory card 275, the image file data are deciphered by using the secret key of the public key cipher system and control for discriminating the enciphered data is performed.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-91744

(P2002-91744A)

(43) 公開日 平成14年3月29日 (2002.3.29)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 0 6 F 3/12		G 0 6 F 3/12	K 2 C 0 6 1
B 4 1 J 5/30		B 4 1 J 5/30	Z 2 C 0 8 7
29/00		G 0 6 K 17/00	S 5 B 0 2 1
G 0 6 K 17/00			D 5 B 0 5 8
		G 0 9 C 1/00	6 4 0 B 5 J 1 0 4
審査請求 未請求 請求項の数36 O L (全 18 頁) 最終頁に続く			

(21) 出願番号 特願2000-285294(P2000-285294)

(22) 出願日 平成12年9月20日 (2000.9.20)

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 笠井 一宏

東京都大田区下丸子3丁目30番2号 キヤノン株式会社内

(72) 発明者 宝木 洋一

東京都大田区下丸子3丁目30番2号 キヤノン株式会社内

(74) 代理人 100081880

弁理士 渡部 敏彦

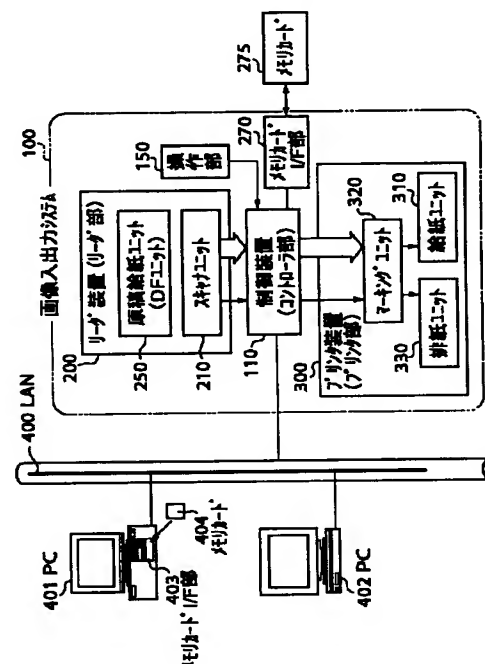
最終頁に続く

(54) 【発明の名称】 画像入力装置、画像出力装置、画像入出力装置、画像データ暗号化方法、画像データ復号化方法及び記憶媒体

(57) 【要約】

【課題】 メモリカード内の画像ファイルデータが第三者によって改ざんされたり不正利用されたりすることを防止し、データの信頼性を向上させることを可能とした画像入力装置、画像出力装置、画像入出力装置、画像データ保存方法、画像データ出力方法及び記憶媒体を提供する。

【解決手段】 制御装置110は、画像ファイルデータをメモリカード275に保存する際、画像ファイルデータを公開鍵暗号方式の公開鍵を用いて暗号化しメモリカード275に保存し、公開鍵暗号方式の公開鍵を用いて暗号化されメモリカード275の画像ファイルデータを出力する際、画像ファイルデータを公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵を用いて復号化し、出力する制御、復号化の際に拡張子に基づき暗号化データを判別する制御を行う。



特開2002-91744

(2)

2

1

【特許請求の範囲】

【請求項1】 メモリカードにアクセス可能な接続手段を備えた画像入力装置であって、
画像データを前記メモリカードに保存する際、前記画像データを公開鍵暗号方式の公開鍵を用いて暗号化し前記メモリカードに保存する制御手段を有することを特徴とする画像入力装置。

【請求項2】 メモリカードにアクセス可能な接続手段を備えた画像入力装置であって、
画像データを前記メモリカードに保存する際、前記画像データを共通鍵暗号方式の秘密鍵を用いて暗号化し前記メモリカードに保存する制御手段を有することを特徴とする画像入力装置。

【請求項3】 メモリカードにアクセス可能な接続手段を備えた画像入力装置であって、
画像データを前記メモリカードに保存する際、前記画像データを共通鍵暗号方式の秘密鍵を用いて暗号化し、前記共通鍵暗号方式の秘密鍵を公開鍵暗号方式の公開鍵を用いて暗号化し、暗号化された前記共通鍵暗号方式の秘密鍵と前記画像データを前記メモリカードに保存する制御手段を有することを特徴とする画像入力装置。

【請求項4】 前記画像データの暗号化に用いる前記公開鍵暗号方式の公開鍵、前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵、前記画像データの暗号化に用いる前記共通鍵暗号方式の秘密鍵の作成或いは選択が可能な操作手段を有することを特徴とする請求項1乃至3の何れかに記載の画像入力装置。

【請求項5】 前記操作手段からは、前記画像データの入手先として、前記画像入力装置、前記メモリカード、前記画像入力装置にデータ通信可能に接続された外部装置の何れかを選択可能であることを特徴とする請求項4記載の画像入力装置。

【請求項6】 メモリカードにアクセス可能な接続手段を備えた画像出力装置であって、
公開鍵暗号方式の公開鍵を用いて暗号化され前記メモリカードに保存されている画像データを画像出力装置内に転送して出力する際、前記画像データを前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵を用いて復号化し、出力する制御手段を有することを特徴とする画像出力装置。

【請求項7】 メモリカードにアクセス可能な接続手段を備えた画像出力装置であって、
共通鍵暗号方式の秘密鍵を用いて暗号化され前記メモリカードに保存されている画像データを画像出力装置内に転送して出力する際、前記画像データを前記共通鍵暗号方式の秘密鍵を用いて復号化し、出力する制御手段を有することを特徴とする画像出力装置。

【請求項8】 メモリカードにアクセス可能な接続手段を備えた画像出力装置であって、
共通鍵暗号方式の秘密鍵を用いて暗号化され且つ前記共

通鍵暗号方式の秘密鍵が公開鍵暗号方式の公開鍵を用いて暗号化され、前記メモリカードに保存されている画像データを画像出力装置内に転送して出力する際、前記暗号化された前記共通鍵暗号方式の秘密鍵を前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵で復号化し、前記画像データを前記復号化された前記共通鍵暗号方式の秘密鍵を用いて復号化し、出力する制御手段を有することを特徴とする画像出力装置。

【請求項9】 前記メモリカードから前記画像出力装置内に転送された画像データの中から前記暗号化された画像データを判別する判別手段を有することを特徴とする請求項6乃至8の何れかに記載の画像出力装置。

【請求項10】 画像データを入力する画像入力手段と、画像データを記録媒体上に印刷し出力する画像出力手段と、メモリカードにアクセス可能な接続手段とを備えた画像入出力装置であって、
画像データを前記メモリカードに保存する際、前記画像データを公開鍵暗号方式の公開鍵を用いて暗号化し前記メモリカードに保存する制御手段を有することを特徴とする画像入出力装置。

【請求項11】 画像データを入力する画像入力手段と、画像データを記録媒体上に印刷し出力する画像出力手段と、メモリカードにアクセス可能な接続手段とを備えた画像入出力装置であって、
画像データを前記メモリカードに保存する際、前記画像データを共通鍵暗号方式の秘密鍵を用いて暗号化し前記メモリカードに保存する制御手段を有することを特徴とする画像入出力装置。

【請求項12】 画像データを入力する画像入力手段と、画像データを記録媒体上に印刷し出力する画像出力手段と、メモリカードにアクセス可能な接続手段とを備えた画像入出力装置であって、
画像データを前記メモリカードに保存する際、前記画像データを共通鍵暗号方式の秘密鍵を用いて暗号化し、前記共通鍵暗号方式の秘密鍵を公開鍵暗号方式の公開鍵を用いて暗号化し、暗号化された前記共通鍵暗号方式の秘密鍵と前記画像データを前記メモリカードに保存する制御手段を有することを特徴とする画像入出力装置。

【請求項13】 前記画像データの暗号化に用いる前記公開鍵暗号方式の公開鍵、前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵、前記画像データの暗号化に用いる前記共通鍵暗号方式の秘密鍵の作成或いは選択が可能な操作手段を有することを特徴とする請求項10乃至12の何れかに記載の画像入出力装置。

【請求項14】 前記操作手段からは、前記画像データの入手先として、前記画像入力手段、前記メモリカード、前記画像入出力装置にデータ通信可能に接続された外部装置の何れかを選択可能であることを特徴とする請求項13記載の画像入出力装置。

【請求項15】 画像データを入力する画像入力手段

10

20

30

40

50

と、画像データを記録媒体上に印刷し出力する画像出力手段と、メモリカードにアクセス可能な接続手段とを備えた画像入出力装置であって、

公開鍵暗号方式の公開鍵を用いて暗号化され前記メモリカードに保存されている画像データを前記画像出力手段に転送して出力する際、前記画像データを前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵を用いて復号化し、出力する制御手段を有することを特徴とする画像入出力装置。

【請求項16】 画像データを入力する画像入力手段と、画像データを記録媒体上に印刷し出力する画像出力手段と、メモリカードにアクセス可能な接続手段とを備えた画像入出力装置であって、共通鍵暗号方式の秘密鍵を用いて暗号化され前記メモリカードに保存されている画像データを前記画像出力手段に転送して出力する際、前記画像データを前記共通鍵暗号方式の秘密鍵を用いて復号化し、出力する制御手段を有することを特徴とする画像入出力装置。

【請求項17】 画像データを入力する画像入力手段と、画像データを記録媒体上に印刷し出力する画像出力手段と、メモリカードにアクセス可能な接続手段とを備えた画像入出力装置であって、共通鍵暗号方式の秘密鍵を用いて暗号化され且つ前記共通鍵暗号方式の秘密鍵が公開鍵暗号方式の公開鍵を用いて暗号化され、前記メモリカードに保存されている画像データを前記画像出力手段に転送して出力する際、前記暗号化された前記共通鍵暗号方式の秘密鍵を前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵で復号化し、前記画像データを前記復号化された前記共通鍵暗号方式の秘密鍵を用いて復号化し、出力する制御手段を有することを特徴とする画像入出力装置。

【請求項18】 前記メモリカードから前記画像出力手段に転送された画像データの中から前記暗号化された画像データを判別する判別手段を有することを特徴とする請求項15乃至17の何れかに記載の画像入出力装置。

【請求項19】 メモリカードにアクセス可能な接続手段を備えた画像入力装置に適用される画像データ暗号化方法であって、画像データを前記メモリカードに保存する際、前記画像データを公開鍵暗号方式の公開鍵を用いて暗号化し前記メモリカードに保存することを特徴とする画像データ暗号化方法。

【請求項20】 メモリカードにアクセス可能な接続手段を備えた画像入力装置に適用される画像データ暗号化方法であって、画像データを前記メモリカードに保存する際、前記画像データを共通鍵暗号方式の秘密鍵を用いて暗号化し前記メモリカードに保存することを特徴とする画像データ暗号化方法。

【請求項21】 メモリカードにアクセス可能な接続手

段を備えた画像入力装置に適用される画像データ暗号化方法であって、

画像データを前記メモリカードに保存する際、前記画像データを共通鍵暗号方式の秘密鍵を用いて暗号化し、前記共通鍵暗号方式の秘密鍵を公開鍵暗号方式の公開鍵を用いて暗号化し、暗号化された前記共通鍵暗号方式の秘密鍵と前記画像データを前記メモリカードに保存することを特徴とする画像データ暗号化方法。

【請求項22】 前記画像データの暗号化に用いる前記公開鍵暗号方式の公開鍵、前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵、前記画像データの暗号化に用いる前記共通鍵暗号方式の秘密鍵の作成或いは選択が可能であることを特徴とする請求項19乃至21の何れかに記載の画像データ暗号化方法。

【請求項23】 前記画像データの入手先として、前記画像入力装置、前記メモリカード、前記画像入力装置にデータ通信可能に接続された外部装置の何れかを選択可能であることを特徴とする請求項22記載の画像データ暗号化方法。

【請求項24】 メモリカードにアクセス可能な接続手段を備えた画像出力装置に適用される画像データ復号化方法であって、公開鍵暗号方式の公開鍵を用いて暗号化され前記メモリカードに保存されている画像データを画像出力装置内に転送して出力する際、前記画像データを前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵を用いて復号化し、出力することを特徴とする画像データ復号化方法。

【請求項25】 メモリカードにアクセス可能な接続手段を備えた画像出力装置に適用される画像データ復号化方法であって、共通鍵暗号方式の秘密鍵を用いて暗号化され前記メモリカードに保存されている画像データを画像出力装置内に転送して出力する際、前記画像データを前記共通鍵暗号方式の秘密鍵を用いて復号化し、出力することを特徴とする画像データ復号化方法。

【請求項26】 メモリカードにアクセス可能な接続手段を備えた画像出力装置に適用される画像データ復号化方法であって、

共通鍵暗号方式の秘密鍵を用いて暗号化され且つ前記共通鍵暗号方式の秘密鍵が公開鍵暗号方式の公開鍵を用いて暗号化され、前記メモリカードに保存されている画像データを画像出力装置内に転送して出力する際、前記暗号化された前記共通鍵暗号方式の秘密鍵を前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵で復号化し、前記画像データを前記復号化された前記共通鍵暗号方式の秘密鍵を用いて復号化し、出力することを特徴とする画像データ復号化方法。

【請求項27】 前記メモリカードから前記画像出力装置内に転送された画像データの中から前記暗号化された

(4)

特開2002-91744

5

6

画像データを判別することを特徴とする請求項24乃至26の何れかに記載の画像データ復号化方法。

【請求項28】 メモリカードにアクセス可能な接続手段を備えた画像入力装置に適用される画像データ暗号化方法を実行するプログラムを記憶したコンピュータにより読み出し可能な記憶媒体であって、

前記画像データ暗号化方法は、画像データを前記メモリカードに保存する際、前記画像データを公開鍵暗号方式の公開鍵を用いて暗号化し前記メモリカードに保存するステップを有することを特徴とする記憶媒体。

【請求項29】 メモリカードにアクセス可能な接続手段を備えた画像入力装置に適用される画像データ暗号化方法を実行するプログラムを記憶したコンピュータにより読み出し可能な記憶媒体であって、

前記画像データ暗号化方法は、画像データを前記メモリカードに保存する際、前記画像データを共通鍵暗号方式の秘密鍵を用いて暗号化し前記メモリカードに保存するステップを有することを特徴とする記憶媒体。

【請求項30】 メモリカードにアクセス可能な接続手段を備えた画像入力装置に適用される画像データ暗号化方法を実行するプログラムを記憶したコンピュータにより読み出し可能な記憶媒体であって、

前記画像データ暗号化方法は、画像データを前記メモリカードに保存する際、前記画像データを共通鍵暗号方式の秘密鍵を用いて暗号化し、前記共通鍵暗号方式の秘密鍵を公開鍵暗号方式の公開鍵を用いて暗号化し、暗号化された前記共通鍵暗号方式の秘密鍵と前記画像データを前記メモリカードに保存するステップを有することを特徴とする記憶媒体。

【請求項31】 前記画像データの暗号化に用いる前記公開鍵暗号方式の公開鍵、前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵、前記画像データの暗号化に用いる前記共通鍵暗号方式の秘密鍵の作成或いは選択が可能なステップを有することを特徴とする請求項28乃至30の何れかに記載の記憶媒体。

【請求項32】 前記画像データの入手先として、前記画像入力装置、前記メモリカード、前記画像入力装置にデータ通信可能に接続された外部装置の何れかを選択可能なステップを有することを特徴とする請求項31記載の記憶媒体。

【請求項33】 メモリカードにアクセス可能な接続手段を備えた画像出力装置に適用される画像データ復号化方法を実行するプログラムを記憶したコンピュータにより読み出し可能な記憶媒体であって、前記画像データ復号化方法は、公開鍵暗号方式の公開鍵を用いて暗号化され前記メモリカードに保存されている画像データを画像出力装置内に転送して出力する際、前記画像データを前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵を用いて復号化し、出力するステップを有することを特徴とする記憶媒体。

10 記憶媒体。

【請求項35】 メモリカードにアクセス可能な接続手段を備えた画像出力装置に適用される画像データ復号化方法を実行するプログラムを記憶したコンピュータにより読み出し可能な記憶媒体であって、

前記画像データ復号化方法は、共通鍵暗号方式の秘密鍵を用いて暗号化され且つ前記共通鍵暗号方式の秘密鍵が公開鍵暗号方式の公開鍵を用いて暗号化され、前記メモリカードに保存されている画像データを画像出力装置内に転送して出力する際、前記暗号化された前記共通鍵暗号方式の秘密鍵を前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵で復号化し、前記画像データを前記復号化された前記共通鍵暗号方式の秘密鍵を用いて復号化し、出力するステップを有することを特徴とする記憶媒体。

【請求項36】 前記メモリカードから前記画像出力装置内に転送された画像データの中から前記暗号化された画像データを判別するステップを有することを特徴とする請求項33乃至35の何れかに記載の記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、画像入力装置、画像出力装置、画像入出力装置、画像データ暗号化方法、画像データ復号化方法及び記憶媒体に関し、特に、メモリカードを利用し画像データを保存する場合に好適な画像入力装置、画像出力装置、画像入出力装置、画像データ暗号化方法、画像データ復号化方法及び記憶媒体に関する。

【0002】

【従来の技術】従来、電子スチルカメラなどといった画像入力システムで作成した画像ファイルデータをメモリカードに保存する方法がある。メモリカードを用いて上記画像ファイルデータを印刷する場合であれば、画像出力システムと接続されたパーソナルコンピュータ（以下PCと略称）、もしくは画像出力システム自体にメモリカードへアクセス可能なインタフェース（以下I/Fと略称）が備えられている場合、上記メモリカードを接続することにより印刷することができる。また、上記画像ファイルデータをPCや電子手帳等に転送する場合であれば、上記メモリカードをメモリカードへアクセス可能なI/Fを備えた被転送装置に接続することにより、容

50

易に画像ファイルデータの授受ができる。

【0003】

【発明が解決しようとする課題】しかしながら、上記従来例の保存方法においては下記のような問題があった。即ち、メモ리카ード内の画像ファイルデータは電子的なデータであるため複製が容易である。そのために、不正複製、不正利用、改ざん等が問題となっている。従って、上記メモ리카ードに保存されている画像ファイルデータの不正利用を防止し、利用者のみが使用できるようにする必要が出てきた。

【0004】そこで、画像入力システムにて画像ファイルデータをメモ리카ードに保存する際、保存対象画像ファイルデータを暗号化することで、上記画像ファイルデータの安全性を向上させることができる。また、電子署名をメモ리카ード内の画像形成装置以外書き込み不可と設定可能なデータ記憶領域に記録することで、更に信頼性が向上する。

【0005】上記の暗号化技術として、IDEA (International Data Encryption Algorithm) 方式などの共通鍵暗号方式や、RSA (Rivest-Shamir-Adelman) 方式などの公開鍵暗号方式を利用したものがある。共通鍵暗号方式は、暗号化及び復号化において同一の秘密鍵を用いるものであり、また、公開鍵暗号方式は、関係者の公開する「公開鍵」と秘密に保持しておく「秘密鍵」という一対の鍵を用いるもので、公開鍵で暗号化したものは秘密鍵でのみ復号化でき、秘密鍵で暗号化したものは公開鍵でのみ復号化できるというものである。図19は上記共通鍵暗号方式及び上記公開鍵暗号方式について概念的に説明したものである。

【0006】秘密鍵暗号は、ソフトウェアでの高速処理が可能であると共に、比較的小規模のハードで高速な暗号を実現しやすいという利点がある。しかし、鍵は暗号化側または復号化側いずれで漏洩してもいけないので、鍵管理を厳重に行うことが必要である。公開鍵暗号方式は、秘密鍵暗号方式と比べ、処理時間が長くなる。しかし、例えば公開鍵暗号方式の公開鍵で暗号化されたものは、その対となる公開鍵暗号方式の秘密鍵でしか復号化できないため、秘密鍵と公開鍵を用いることで鍵の管理を容易にすることができる。

【0007】そこで、従来から、鍵の管理を容易にしながら、上記メモ리카ード内の画像ファイルデータの不正複製、不正利用、改ざんを防止する技術が要望されていた。

【0008】本発明は、上述した点に鑑みなされたものであり、メモ리카ード内の画像ファイルデータが第三者によって改ざんされたり不正利用されたりすることを防止し、データの信頼性を向上させることを可能とした画像入力装置、画像出力装置、画像入出力装置、画像データ暗号化方法、画像データ復号化方法及び記憶媒体を提供することを第一の目的とする。

【0009】また、本発明は、上述した点に鑑みなされたものであり、出力するデータの信頼性を向上させることを可能とした画像入力装置、画像出力装置、画像入出力装置、画像データ暗号化方法、画像データ復号化方法及び記憶媒体を提供することを第二の目的とする。

【0010】また、本発明は、上述した点に鑑みなされたものであり、ユーザがより容易にデータの復号化を行うことを可能とした画像入力装置、画像出力装置、画像入出力装置、画像データ暗号化方法、画像データ復号化方法及び記憶媒体を提供することを第三の目的とする。

【0011】

【課題を解決するための手段】上記目的を達成するため、請求項1の発明は、メモ리카ードにアクセス可能な接続手段を備えた画像入力装置であって、画像データを前記メモ리카ードに保存する際、前記画像データを公開鍵暗号方式の公開鍵を用いて暗号化し前記メモ리카ードに保存する制御手段を有することを特徴とする。

【0012】上記目的を達成するため、請求項2の発明は、メモ리카ードにアクセス可能な接続手段を備えた画像入力装置であって、画像データを前記メモ리카ードに保存する際、前記画像データを共通鍵暗号方式の秘密鍵を用いて暗号化し前記メモ리카ードに保存する制御手段を有することを特徴とする。

【0013】上記目的を達成するため、請求項3の発明は、メモ리카ードにアクセス可能な接続手段を備えた画像入力装置であって、画像データを前記メモ리카ードに保存する際、前記画像データを共通鍵暗号方式の秘密鍵を用いて暗号化し、前記共通鍵暗号方式の秘密鍵を公開鍵暗号方式の公開鍵を用いて暗号化し、暗号化された前記共通鍵暗号方式の秘密鍵と前記画像データを前記メモ리카ードに保存する制御手段を有することを特徴とする。

【0014】上記目的を達成するため、請求項4の発明は、前記画像データの暗号化に用いる前記公開鍵暗号方式の公開鍵、前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵、前記画像データの暗号化に用いる前記共通鍵暗号方式の秘密鍵の作成或いは選択が可能な操作手段を有することを特徴とする。

【0015】上記目的を達成するため、請求項5の発明は、前記操作手段からは、前記画像データの入手先として、前記画像入力装置、前記メモ리카ード、前記画像入力装置にデータ通信可能に接続された外部装置の何れかを選択可能であることを特徴とする。

【0016】上記目的を達成するため、請求項6の発明は、メモ리카ードにアクセス可能な接続手段を備えた画像出力装置であって、公開鍵暗号方式の公開鍵を用いて暗号化され前記メモ리카ードに保存されている画像データを画像出力装置内に転送して出力する際、前記画像データを前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵を用いて復号化し、出力する制御手段を

10

20

30

40

50

(6)

特開2002-91744

9

10

有することを特徴とする。

【0017】上記目的を達成するため、請求項7の発明は、メモ리카ードにアクセス可能な接続手段を備えた画像出力装置であって、共通鍵暗号方式の秘密鍵を用いて暗号化され前記メモ리카ードに保存されている画像データを画像出力装置内に転送して出力する際、前記画像データを前記共通鍵暗号方式の秘密鍵を用いて復号化し、出力する制御手段を有することを特徴とする。

【0018】上記目的を達成するため、請求項8の発明は、メモ리카ードにアクセス可能な接続手段を備えた画像出力装置であって、共通鍵暗号方式の秘密鍵を用いて暗号化され且つ前記共通鍵暗号方式の秘密鍵が公開鍵暗号方式の公開鍵を用いて暗号化され、前記メモ리카ードに保存されている画像データを画像出力装置内に転送して出力する際、前記暗号化された前記共通鍵暗号方式の秘密鍵を前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵で復号化し、前記画像データを前記復号化された前記共通鍵暗号方式の秘密鍵を用いて復号化し、出力する制御手段を有することを特徴とする。

【0019】上記目的を達成するため、請求項9の発明は、前記メモ리카ードから前記画像出力装置内に転送された画像データの中から前記暗号化された画像データを判別する判別手段を有することを特徴とする。

【0020】上記目的を達成するため、請求項10の発明は、画像データを入力する画像入力手段と、画像データを記録媒体上に印刷し出力する画像出力手段と、メモ리카ードにアクセス可能な接続手段とを備えた画像入出力装置であって、画像データを前記メモ리카ードに保存する際、前記画像データを公開鍵暗号方式の公開鍵を用いて暗号化し前記メモ리카ードに保存する制御手段を有することを特徴とする。

【0021】上記目的を達成するため、請求項11の発明は、画像データを入力する画像入力手段と、画像データを記録媒体上に印刷し出力する画像出力手段と、メモ리카ードにアクセス可能な接続手段とを備えた画像入出力装置であって、画像データを前記メモ리카ードに保存する際、前記画像データを共通鍵暗号方式の秘密鍵を用いて暗号化し前記メモ리카ードに保存する制御手段を有することを特徴とする。

【0022】上記目的を達成するため、請求項12の発明は、画像データを入力する画像入力手段と、画像データを記録媒体上に印刷し出力する画像出力手段と、メモ리카ードにアクセス可能な接続手段とを備えた画像入出力装置であって、画像データを前記メモ리카ードに保存する際、前記画像データを共通鍵暗号方式の秘密鍵を用いて暗号化し、前記共通鍵暗号方式の秘密鍵を公開鍵暗号方式の公開鍵を用いて暗号化し、暗号化された前記共通鍵暗号方式の秘密鍵と前記画像データを前記メモ리카ードに保存する制御手段を有することを特徴とする。

【0023】上記目的を達成するため、請求項13の発

明は、前記画像データの暗号化に用いる前記公開鍵暗号方式の公開鍵、前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵、前記画像データの暗号化に用いる前記共通鍵暗号方式の秘密鍵の作成或いは選択が可能な操作手段を有することを特徴とする。

【0024】上記目的を達成するため、請求項14の発明は、前記操作手段からは、前記画像データの入手先として、前記画像入力手段、前記メモ리카ード、前記画像入出力装置にデータ通信可能に接続された外部装置の何れかを選択可能であることを特徴とする。

【0025】上記目的を達成するため、請求項15の発明は、画像データを入力する画像入力手段と、画像データを記録媒体上に印刷し出力する画像出力手段と、メモ리카ードにアクセス可能な接続手段とを備えた画像入出力装置であって、公開鍵暗号方式の公開鍵を用いて暗号化され前記メモ리카ードに保存されている画像データを前記画像出力手段に転送して出力する際、前記画像データを前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵を用いて復号化し、出力する制御手段を有することを特徴とする。

【0026】上記目的を達成するため、請求項16の発明は、画像データを入力する画像入力手段と、画像データを記録媒体上に印刷し出力する画像出力手段と、メモ리카ードにアクセス可能な接続手段とを備えた画像入出力装置であって、共通鍵暗号方式の秘密鍵を用いて暗号化され前記メモ리카ードに保存されている画像データを前記画像出力手段に転送して出力する際、前記画像データを前記共通鍵暗号方式の秘密鍵を用いて復号化し、出力する制御手段を有することを特徴とする。

【0027】上記目的を達成するため、請求項17の発明は、画像データを入力する画像入力手段と、画像データを記録媒体上に印刷し出力する画像出力手段と、メモ리카ードにアクセス可能な接続手段とを備えた画像入出力装置であって、共通鍵暗号方式の秘密鍵を用いて暗号化され且つ前記共通鍵暗号方式の秘密鍵が公開鍵暗号方式の公開鍵を用いて暗号化され、前記メモ리카ードに保存されている画像データを前記画像出力手段に転送して出力する際、前記暗号化された前記共通鍵暗号方式の秘密鍵を前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵で復号化し、前記画像データを前記復号化された前記共通鍵暗号方式の秘密鍵を用いて復号化し、出力する制御手段を有することを特徴とする。

【0028】上記目的を達成するため、請求項18の発明は、前記メモ리카ードから前記画像出力手段に転送された画像データの中から前記暗号化された画像データを判別する判別手段を有することを特徴とする。

【0029】上記目的を達成するため、請求項19の発明は、メモ리카ードにアクセス可能な接続手段を備えた画像入力装置に適用される画像データ暗号化方法であって、画像データを前記メモ리카ードに保存する際、前記

50

(7)

特開2002-91744

11

画像データを公開鍵暗号方式の公開鍵を用いて暗号化し前記メモリカードに保存することを特徴とする。

【0030】上記目的を達成するため、請求項20の発明は、メモリカードにアクセス可能な接続手段を備えた画像入力装置に適用される画像データ暗号化方法であって、画像データを前記メモリカードに保存する際、前記画像データを共通鍵暗号方式の秘密鍵を用いて暗号化し前記メモリカードに保存することを特徴とする。

【0031】上記目的を達成するため、請求項21の発明は、メモリカードにアクセス可能な接続手段を備えた画像入力装置に適用される画像データ暗号化方法であって、画像データを前記メモリカードに保存する際、前記画像データを共通鍵暗号方式の秘密鍵を用いて暗号化し、前記共通鍵暗号方式の秘密鍵を公開鍵暗号方式の公開鍵を用いて暗号化し、暗号化された前記共通鍵暗号方式の秘密鍵と前記画像データを前記メモリカードに保存することを特徴とする。

【0032】上記目的を達成するため、請求項22の発明は、前記画像データの暗号化に用いる前記公開鍵暗号方式の公開鍵、前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵、前記画像データの暗号化に用いる前記共通鍵暗号方式の秘密鍵の作成或いは選択が可能であることを特徴とする。

【0033】上記目的を達成するため、請求項23の発明は、前記画像データの入手先として、前記画像入力装置、前記メモリカード、前記画像入力装置にデータ通信可能に接続された外部装置の何れかを選択可能であることを特徴とする。

【0034】上記目的を達成するため、請求項24の発明は、メモリカードにアクセス可能な接続手段を備えた画像出力装置に適用される画像データ復号化方法であって、公開鍵暗号方式の公開鍵を用いて暗号化され前記メモリカードに保存されている画像データを画像出力装置内に転送して出力する際、前記画像データを前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵を用いて復号化し、出力することを特徴とする。

【0035】上記目的を達成するため、請求項25の発明は、メモリカードにアクセス可能な接続手段を備えた画像出力装置に適用される画像データ復号化方法であって、共通鍵暗号方式の秘密鍵を用いて暗号化され前記メモリカードに保存されている画像データを画像出力装置内に転送して出力する際、前記画像データを前記共通鍵暗号方式の秘密鍵を用いて復号化し、出力することを特徴とする。

【0036】上記目的を達成するため、請求項26の発明は、メモリカードにアクセス可能な接続手段を備えた画像出力装置に適用される画像データ復号化方法であって、共通鍵暗号方式の秘密鍵を用いて暗号化され且つ前記共通鍵暗号方式の秘密鍵が公開鍵暗号方式の公開鍵を用いて暗号化され、前記メモリカードに保存されている

12

画像データを画像出力装置内に転送して出力する際、前記暗号化された前記共通鍵暗号方式の秘密鍵を前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵で復号化し、前記画像データを前記復号化された前記共通鍵暗号方式の秘密鍵を用いて復号化し、出力することを特徴とする。

【0037】上記目的を達成するため、請求項27の発明は、前記メモリカードから前記画像出力装置内に転送された画像データの中から前記暗号化された画像データを判別することを特徴とする。

【0038】上記目的を達成するため、請求項28の発明は、メモリカードにアクセス可能な接続手段を備えた画像入力装置に適用される画像データ暗号化方法を実行するプログラムを記憶したコンピュータにより読み出し可能な記憶媒体であって、前記画像データ暗号化方法は、画像データを前記メモリカードに保存する際、前記画像データを公開鍵暗号方式の公開鍵を用いて暗号化し前記メモリカードに保存するステップを有することを特徴とする。

【0039】上記目的を達成するため、請求項29の発明は、メモリカードにアクセス可能な接続手段を備えた画像入力装置に適用される画像データ暗号化方法を実行するプログラムを記憶したコンピュータにより読み出し可能な記憶媒体であって、前記画像データ暗号化方法は、画像データを前記メモリカードに保存する際、前記画像データを共通鍵暗号方式の秘密鍵を用いて暗号化し前記メモリカードに保存するステップを有することを特徴とする。

【0040】上記目的を達成するため、請求項30の発明は、メモリカードにアクセス可能な接続手段を備えた画像入力装置に適用される画像データ暗号化方法を実行するプログラムを記憶したコンピュータにより読み出し可能な記憶媒体であって、前記画像データ暗号化方法は、画像データを前記メモリカードに保存する際、前記画像データを共通鍵暗号方式の秘密鍵を用いて暗号化し、前記共通鍵暗号方式の秘密鍵を公開鍵暗号方式の公開鍵を用いて暗号化し、暗号化された前記共通鍵暗号方式の秘密鍵と前記画像データを前記メモリカードに保存するステップを有することを特徴とする。

【0041】上記目的を達成するため、請求項31の発明は、前記画像データの暗号化に用いる前記公開鍵暗号方式の公開鍵、前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵、前記画像データの暗号化に用いる前記共通鍵暗号方式の秘密鍵の作成或いは選択が可能なるステップを有することを特徴とする。

【0042】上記目的を達成するため、請求項32の発明は、前記画像データの入手先として、前記画像入力装置、前記メモリカード、前記画像入力装置にデータ通信可能に接続された外部装置の何れかを選択可能なステップを有することを特徴とする。

(8)

特開2002-91744

13

【0043】上記目的を達成するため、請求項33の発明は、メモ리카ードにアクセス可能な接続手段を備えた画像出力装置に適用される画像データ復号化方法を実行するプログラムを記憶したコンピュータにより読み出し可能な記憶媒体であって、前記画像データ復号化方法は、公開鍵暗号方式の公開鍵を用いて暗号化され前記メモ리카ードに保存されている画像データを画像出力装置内に転送して出力する際、前記画像データを前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵を用いて復号化し、出力するステップを有することを特徴とする。

【0044】上記目的を達成するため、請求項34の発明は、メモ리카ードにアクセス可能な接続手段を備えた画像出力装置に適用される画像データ復号化方法を実行するプログラムを記憶したコンピュータにより読み出し可能な記憶媒体であって、前記画像データ復号化方法は、共通鍵暗号方式の秘密鍵を用いて暗号化され前記メモ리카ードに保存されている画像データを画像出力装置内に転送して出力する際、前記画像データを前記共通鍵暗号方式の秘密鍵を用いて復号化し、出力するステップ

【0045】上記目的を達成するため、請求項35の発明は、メモ리카ードにアクセス可能な接続手段を備えた画像出力装置に適用される画像データ復号化方法を実行するプログラムを記憶したコンピュータにより読み出し可能な記憶媒体であって、前記画像データ復号化方法は、共通鍵暗号方式の秘密鍵を用いて暗号化され且つ前記共通鍵暗号方式の秘密鍵が公開鍵暗号方式の公開鍵を用いて暗号化され、前記メモ리카ードに保存されている画像データを画像出力装置内に転送して出力する際、前記暗号化された前記共通鍵暗号方式の秘密鍵を前記公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵で復号化し、前記画像データを前記復号化された前記共通鍵暗号方式の秘密鍵を用いて復号化し、出力するステップを有することを特徴とする。

【0046】上記目的を達成するため、請求項36の発明は、前記メモ리카ードから前記画像出力装置内に転送された画像データの中から前記暗号化された画像データを判別するステップを有することを特徴とする。

【0047】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて詳細に説明する。

【0048】〔第1の実施の形態〕図1は本発明の第1の実施の形態に係る画像入出力システムの全体構成を示すブロック図である。本発明の第1の実施の形態に係る画像入出力システム100は、制御装置（コントローラ部）110（制御手段、判別手段）、操作部150（操作手段）、スキャナユニット210・原稿給紙ユニット（DFユニット）250を有するリーダ装置（リーダ部）200（画像入力手段）、メモ리카ードインタフェ

14

ース（I/F）部270（接続手段）、給紙ユニット310・マーキングユニット320・排紙ユニット330を有するプリンタ装置（プリンタ部）300（画像出力手段）を備えている。図中275はメモ리카ード、400はLAN等からなるネットワーク、401、402はPCからなるホストコンピュータである。

【0049】上記構成を詳述すると、リーダ部200は、本画像入出力システムにおける画像入力システムを構成するものであり、原稿画像を光学的に読み取り、画像データに変換する。リーダ部200は、原稿を読み取るための機能を持つスキャナユニット210と、原稿用紙を搬送するための機能を持つ原稿給紙ユニット250とから構成される。

【0050】プリンタ部300は、本画像入出力システムにおける画像出力システムを構成するものであり、記録紙を搬送し、その上に画像データを可視画像として印字して装置外に排紙する。プリンタ部300は、複数種類の記録紙カセットを持つ給紙ユニット310と、画像データを記録紙に転写、定着させる機能を持つマーキングユニット320と、印字された記録紙をソート、ステイブルして機外へ出力する機能を持つ排紙ユニット330とから構成される。

【0051】制御装置110は、リーダ部200、プリンタ部300、メモ리카ードI/F部270と電氣的に接続され、更にネットワーク400を介してホストコンピュータ401、402と接続されている。制御装置110は、リーダ部200を制御して原稿の画像データを読み込み、プリンタ部300を制御して画像データを記録紙に印字出力するコピー機能を提供する。

【0052】また、制御装置110は、リーダ部200から読み取った画像データをコードデータに変換し、ネットワーク400を介してホストコンピュータ401、402へ送信するスキャナ機能、メモ리카ードI/F部270から読み取った画像データをネットワーク400を介してホストコンピュータ401、402へ送信するデータ転送機能、ホストコンピュータ401、402からネットワーク400を介して受信したコードデータを画像データに変換し、プリンタ部300に出力するプリンタ機能を提供する。また、制御装置110は、プログラムに基づき後述の各フローチャートに示す処理を実行する。

【0053】メモ리카ードI/F部270は、メモ리카ード275に蓄積されているデータを読み取ったり、制御装置110に蓄積されているデータをメモ리카ード275に書き込んだりする。操作部150は、制御装置110に接続されると共に、例えば液晶タッチパネルから構成されており、本画像入出力システムを操作するためのユーザI/Fを提供する。

【0054】図2は本発明の第1の実施の形態に係る画像入出力システム100のリーダ部200及びプリンタ

50

(9)

15

部300の内部構造を示す構成図である。本発明の第1の実施の形態に係る画像入出力システムのリーダ部200は、ブラテンガラス211、ランプ212・ミラー214を有する光学ユニット213、ミラー215、ミラー216、レンズ217、CCDイメージセンサ（以下CCDと略称）218、原稿給送ユニット250を備え、プリンタ部300は、カセット311、カセット312、レーザドライバ321、レーザ発光部322、感光ドラム323、現像器324、転写部325、定着部326、排出ローラ327、フラップ328、再給紙搬送路329、排紙ユニット330を備えている。

【0055】上記構成を動作と共に詳述すると、リーダ部200の原稿給送ユニット250は、原稿を先頭順に1枚ずつブラテンガラス211上へ給送し、原稿の読み取り動作終了後、ブラテンガラス211上の原稿を排出するものである。原稿がブラテンガラス211上に搬送されると、光学ユニット213のランプ212を点灯し、そして光学ユニット213の移動を開始させて、原稿を露光走査する。この時の原稿からの反射光は、ミラー214、215、216及びレンズ217によってCCD218へ導かれる。このように走査された原稿の画像はCCD218によって読み取られる。CCD218から出力される画像データは所定の処理が施された後、制御装置110へ転送される。

【0056】プリンタ部300のレーザドライバ321は、レーザ発光部322を駆動するものであり、制御装置110から出力された画像データに応じたレーザ光をレーザ発光部322に発光させる。このレーザ光は感光ドラム323に照射され、感光ドラム323にはレーザ光に応じた潜像が形成される。この感光ドラム323の潜像の部分には現像器324によって現像剤が付着される。そして、レーザ光の照射開始と同期したタイミングで、カセット311及びカセット312の何れかから記録紙を給紙して転写部325へ搬送し、感光ドラム323に付着された現像剤を記録紙に転写する。

【0057】現像剤の乗った記録紙は定着部326に搬送され、定着部326の熱と圧力により現像剤は記録紙に定着される。定着部326を通過した記録紙は排出ローラ327によって排出され、排紙ユニット330は排出された記録紙を束ねて記録紙の仕分けをしたり、仕分けされた記録紙のステイブルを行う。また、両面記録が設定されている場合は、排出ローラ327の配設箇所まで記録紙を搬送した後、排出ローラ327の回転方向を逆転させ、フラップ328によって再給紙搬送路329へ導く。再給紙搬送路329へ導かれた記録紙は上述したタイミングで転写部325へ給紙される。

【0058】図4は本発明の第1の実施の形態に係るメモ리카ード275のメモリマップの一例を示す説明図である。メモ리카ード275には、画像ファイルデータ及びプロパティファイルが保存されている。プロパティ

特開2002-91744

16

ファイルは、基本的にASCIIコードのみで使用したText形式により記載されており、プリントジョブ毎に指定情報が完結する記述となっている。また、プロパティファイルは、メモ리카ード275内に1つ存在し、対象となる画像ファイルデータは保存場所を問わない。更に、このプロパティファイルは、対象装置以外書き込み不可と設定可能なデータ記憶領域を持つ。

【0059】図18は本発明の画像データ暗号化方法、画像データ復号化方法を実行するプログラム及び関連データが記憶媒体から装置に供給される概念例を示す説明図である。本発明の画像データ暗号化方法、画像データ復号化方法を実行するプログラム及び関連データは、フロッピディスクやCD-ROM等の記憶媒体181を装置182に装備された記憶媒体ドライブ挿入口183に挿入することで供給される。その後、本発明の画像データ暗号化方法、画像データ復号化方法を実行するプログラム及び関連データを記憶媒体181から一旦ハードディスクにインストールしハードディスクからRAMにロードするか、或いはハードディスクにインストールせずに直接RAMにロードすることで、プログラム及び関連データを実行することが可能となる。

【0060】この場合、本発明の第1～第2の実施の形態に係る画像入出力システムにおいて、本発明の画像データ暗号化方法、画像データ復号化方法を実行するプログラムを実行する場合は、例えば上記図18を参照して説明したような手順で画像入出力システムに当該プログラム及び関連データを供給するか、或いは画像入出力システムに予め当該プログラム及び関連データを格納しておくことで、プログラム実行が可能となる。

【0061】図17は本発明の画像データ暗号化方法、画像データ復号化方法を実行するプログラム及び関連データを記憶した記憶媒体の記憶内容の構成例を示す説明図である。記憶媒体は、例えばボリューム情報171、ディレクトリ情報172、プログラム実行ファイル173、プログラム関連データファイル174等の記憶内容で構成される。本発明の画像データ暗号化方法、画像データ復号化方法を実行するプログラムは、後述の各フローチャートに基づきプログラムコード化されたものである。

【0062】次に、上記の如く構成された本発明の第1の実施の形態に係る画像ファイルデータを暗号化したメモ리카ード利用画像入出力システムの制御手順の一例について、図1～図11を参照しながら詳細に説明する。第1の実施の形態の画像入力システムとしては、上記図1に示したような画像入出力システムのリーダ部の他に、電子スチルカメラ、スキャナなどが考えられる。第1の実施の形態では、画像入力方法及び画像出力方法として上記図1の画像入出力システムを用いる。

【0063】画像ファイルデータを暗号化しメモ리카ード275に保存させる場合、ユーザが画像入出力シス

10

20

30

40

50

(10)

特開2002-91744

17

ム100の操作部150に装備されている「画像ファイルデータをメモリカードに保存」というキーを押下することにより、画像ファイルデータのメモリカード275への保存制御が開始される。ユーザは画像ファイルデータの入手先を操作部150にて指示し（ステップS1001）、画像入出力システム100はその指示に従ってユーザが作成した画像ファイルを、リーダ部200やネットワーク400を介したホストコンピュータ401、402より制御装置110に取り込む（ステップS1002）。図6は操作部150に表示される意向選択の一例を示す説明図である。本例は、画像ファイルの入手先として、「メモリカード」、「ホストコンピュータ」、「リーダ部」から選択する例である。尚、意向選択は図6に限定されるものではない。

【0064】ユーザは、画像入出力システム100にて取り込んだ画像ファイルデータを暗号化しメモリカード275に保存するかどうかを操作部150にて指示する（ステップS1003）。図7は操作部150に表示される意向選択の一例を示す説明図である。本例は、保存するデータの保存形態として、「署名付保存（画像）」、「署名付保存（画像・プロパティファイル）」、「署名なし保存」から選択する例である。尚、意向選択は図7に限定されるものではない。

【0065】画像ファイルデータを暗号化せずにメモリカード275に保存する場合は、そのまま画像ファイルデータ及びプロパティファイルをメモリカード275に保存する。他方、画像ファイルデータを暗号化する場合は、図3に示すように、画像ファイルデータを「公開鍵暗号方式の公開鍵」で暗号化する。この公開鍵は、のちに出力する画像出力システム固有の鍵、もしくはユーザ自身が作成した鍵などを任意に選択でき、また、その公開鍵と対になる「公開鍵暗号方式の秘密鍵」は厳重に管理されなければならない。尚、画像ファイルデータを共通鍵暗号方式の秘密鍵を用いて暗号化することも可能である。

【0066】上記画像ファイルデータを暗号化するための公開鍵を操作部150で選択・決定した後（ステップS1004）、制御装置110は上記画像ファイルデータを該公開鍵で暗号化する（ステップS1005）。図8は操作部150に表示される意向選択の一例を示す説明図である。本例は、使用する鍵として、「機器固有鍵」、「登録済みユーザ鍵」、「ユーザ鍵の新規作成」から選択する例である。尚、意向選択は図8に限定されるものではない。画像ファイルデータやプロパティファイルは、ユーザの選択によりメモリカード275の対象装置以外書き込み不可領域に保存することもできる（ステップS1008、ステップS1010）。

【0067】次に、メモリカード275に保存された画像ファイルデータ及びプロパティファイルを画像出力システムにて復号化し、出力する方法を述べる。メモリカ

18

ード275が画像入出力システム100のメモリカードI/F部270と接続された状態で制御が行われ、ユーザが操作部150に装備されているメモリカード内画像データキーを押下することにより、画像ファイルデータの復号・出力制御が開始される。制御装置110は、メモリカードI/F部270を介してメモリカード275に、画像入出力システム100にて出力するデータが蓄積されているかどうかを確認する（ステップS1101）。

【0068】例えばメモリカード275内には、上記図4のメモリマップに示すように、暗号化された画像ファイルデータ（pic1, pgp）、暗号化されていない画像ファイルデータ（pic2, jpg）、そしてプロパティファイル（prop, txt）とが蓄積されており、それらのデータをメモリカードI/F部270を介して制御装置110に転送する（ステップS1102）。データが蓄積されていない場合は、この制御を終了する。

【0069】次に、制御装置110は転送された各データについて拡張子を判別することにより、暗号化されているかどうか検証する（ステップS1103）。暗号化ファイルが存在しなければ、メモリカード275中には暗号化データが存在していないと判断し、復号化の処理を行わず、プロパティファイルに記述されたプリントジョブ情報に基づいて画像を出力する（ステップS1107）。図5はプリントジョブ情報の一例を示す説明図である。「pic1, jpg, A4, SS, 1P」は、画像（pic1, jpg）をA4用紙（A4）に片面印刷（SS）で1部（1P）印刷するというものである。

【0070】暗号化データが存在するならば、そのデータを復号化するための「公開鍵暗号方式の秘密鍵」が画像入出力システム100に存在するかを確認し（ステップS1104）、該秘密鍵が存在しなければ、操作部150に「秘密鍵が存在しない」というメッセージを表示させる。このときユーザは、該当する秘密鍵をシステムに格納させる必要がある（ステップS1105）。秘密鍵がシステムに存在するならば、図3に示すように、秘密鍵を用いて暗号化データを復号化し（ステップS1106）、プロパティファイルに記述されたプリントジョブ情報に基づいて画像出力処理を行う（ステップS1107）。

【0071】以上説明したように、本発明の第1の実施の形態に係る画像入出力システムによれば、制御装置110は、画像ファイルデータをメモリカード275に保存する際、画像ファイルデータを公開鍵暗号方式の公開鍵を用いて暗号化しメモリカード275に保存し、公開鍵暗号方式の公開鍵を用いて暗号化されメモリカード275に保存されている画像ファイルデータを読み出して出力する際、画像ファイルデータを公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵を用いて復号化

50

(11)

特開2002-91744

19

し、出力する制御を行うと共に、復号化の際に拡張子に基づき暗号化データを判別する制御を行うため、下記のような効果を奏する。

【0072】画像入力システムにおいて作成されたデータをメモ리카ード275に保存する際、公開鍵暗号方式の公開鍵もしくは共通鍵暗号方式の秘密鍵を用いて暗号化することにより、上記データが第三者によって改ざんされたり不正利用されたりすることを防止でき、データの信頼性を向上させることができるという効果を奏する。

【0073】また、メモ리카ード275に保存されたデータを画像出力システムにて出力する際、公開鍵暗号方式公開鍵で暗号化されたデータを公開鍵暗号方式秘密鍵で復号化することで、出力する上記データの信頼性を向上させることができるという効果を奏する。

【0074】また、暗号化されたデータを復号化する際、暗号化されたデータと暗号化されていないデータとを判別することで、ユーザはより容易にデータの復号化を行うことが可能となる効果を奏する。

【0075】〔第2の実施の形態〕本発明の第2の実施の形態に係る画像入出力システム100は、上記第1の実施の形態と同様に、制御装置（コントローラ部）110、操作部150、スキャナユニット210・原稿給紙ユニット（DFユニット）250を有するリーダ装置（リーダ部）200、メモ리카ードI/F部270、給紙ユニット310・マーキングユニット320・排紙ユニット330を有するプリンタ装置（プリンタ部）300を備えている（上記図1参照）。

【0076】また、本発明の第2の実施の形態に係る画像入出力システム100のリーダ部200は、上記第1の実施の形態と同様に、ブラテンガラス211、ランプ212・ミラー214を有する光学ユニット213、ミラー215、ミラー216、レンズ217、CCDイメージセンサ（以下CCDと略称）218、原稿給送ユニット250を備え、プリンタ部300は、カセット311、カセット312、レーザドライバ321、レーザ発光部322、感光ドラム323、現像器324、転写部325、定着部326、排出ローラ327、フラップ328、再給紙搬送路329、排紙ユニット330を備えている（上記図2参照）。

【0077】上記第1の実施の形態においては、上記図3に示したように画像ファイルデータを公開鍵暗号方式でのみ暗号化していた。この方法は、（1）暗号鍵と復号鍵が異なるため安全性が高い、（2）暗号化または復号化するために相手に公開鍵を公開するだけでよいので安全性が高い、という利点がある。

【0078】しかし、暗号化処理速度が遅く、共通鍵暗号方式と比べると2桁以上多くかかるという問題がある。そのため、画像ファイルデータのようなデータ量が大きいものを公開鍵暗号方式で暗号化するのはあまりふ

20

さわしいとは言えない。一方、共通鍵暗号方式では、暗号化処理の速度は速いが、暗号鍵と復号鍵が同一であるため安全性は低いという欠点がある。

【0079】そこで、本発明の第2の実施の形態は、これら公開鍵暗号方式と共通鍵暗号方式との両方を用いることで、より安全性が高く、実用性がある暗号化方法を取るようにしたものである。

【0080】公開鍵暗号方式と共通鍵暗号方式の両方を用いた画像入出力システムの暗号化についての概略図を図12に示す。この図12に示されているように、画像ファイルデータを暗号化してメモ리카ード275に保存する時、画像ファイルデータを「共通鍵暗号方式の秘密鍵」で暗号化し、その「共通鍵暗号方式の秘密鍵」を「公開鍵暗号方式の公開鍵」で暗号化する。そして、暗号化された「共通鍵暗号方式の秘密鍵」と画像ファイルデータをメモ리카ード275に保存する。メモ리카ード275にあるデータを復号化し出力するときは、「公開鍵暗号方式の公開鍵」で暗号化された「共通鍵暗号方式の秘密鍵」を「公開鍵暗号方式の秘密鍵」で復号化し、その復号化された「共通鍵暗号方式の秘密鍵」を用いて暗号化された画像ファイルデータを復号化する。そして、その画像ファイルデータを出力する。

【0081】次に、上記の如く構成された本発明の第2の実施の形態に係る公開鍵暗号方式と共通鍵暗号方式の両方を用いた画像入出力システムの暗号化及び復号化について、図1～図2、図5～図8、図12～図16を参照しながら詳細に説明する。第2の実施の形態の画像入力システムとしては、上記第1の実施の形態と同様に、上記図1に示したような画像入出力システムのリーダ部の他に、電子スチルカメラ、スキャナなどが考えられる。第2の実施の形態においても、画像入力方法及び画像出力方法として上記図1の画像入出力システムを用いる。

【0082】画像ファイルデータを暗号化しメモ리카ード275に保存させる処理において、ユーザが画像入出力システム100の操作部150に装備されている「画像ファイルデータをメモ리카ードに保存」というキーを押下することにより、画像ファイルデータのメモ리카ード275への保存制御が開始される。ユーザは画像ファイルデータの入手先を操作部150にて指示し（ステップS1201）、画像入出力システム100はその指示に従ってユーザが作成した画像ファイルを、リーダ部200やネットワーク400を介したホストコンピュータ401、402より制御装置110に取り込む（ステップS1202）。図6は操作部150に表示される意向選択の一例を示す説明図である。本例は、画像ファイルの入手先として、「メモ리카ード」、「ホストコンピュータ」、「リーダ部」から選択する例である。尚、意向選択は図6に限定されるものではない。

【0083】ユーザは、画像入出力システム100にて

50

(12)

特開2002-91744

21

取り込んだ画像ファイルデータを暗号化しメモリカード275に保存するかどうかを操作部150にて指示する(ステップS1203)。図7は操作部150に表示される意向選択の一例を示す説明図である。本例は、保存するデータの保存形態として、「署名付保存(画像)」、「署名付保存(画像・プロパティファイル)」、「署名なし保存」から選択する例である。尚、意向選択は図7に限定されるものではない。

【0084】画像ファイルデータを暗号化せずにメモリカード275に保存する場合は、そのまま画像ファイルデータ及びプロパティファイルをメモリカード275に保存する。他方、画像ファイルデータを暗号化するためには、図12に示すように、画像ファイルデータを暗号化するために用いる「共通鍵暗号方式秘密鍵」、及び共通鍵暗号方式秘密鍵を暗号化する「公開鍵暗号方式公開鍵」の2つを操作部150で選択・決定する(ステップS1204)。図8は操作部150に表示される意向選択の一例を示す説明図である。本例は、使用する鍵として、「機器固有鍵」、「登録済みユーザ鍵」、「ユーザ鍵の新規作成」から選択する例である。尚、意向選択は

【0085】制御装置110は上記画像ファイルデータを上記選択した共通鍵暗号方式秘密鍵で暗号化し(ステップS1205)、上記共通鍵暗号方式秘密鍵を上記公開鍵暗号方式公開鍵で暗号化する(ステップS1206)。この公開鍵は、のちに出力する画像出力システム固有の鍵、もしくはユーザ自身が作成した鍵などであり、その公開鍵暗号方式公開鍵と対となる公開鍵暗号方式秘密鍵は厳重に管理されなければならない。

【0086】また、プロパティファイルも公開鍵暗号方式公開鍵で暗号化するならば暗号化する(ステップS1208)。これらのデータやプロパティファイルをメモリカード275に保存し、画像ファイルデータをメモリカード275に保存する制御を終了する。画像ファイルデータやプロパティファイルは、ユーザの選択によりメモリカード275の対象装置以外書き込み不可領域に保存することもできる(ステップS1211)。

【0087】次に、メモリカード275に保存された画像ファイルデータ及びプロパティファイルを画像出力システムにて復号化し、出力する方法を述べる。メモリカード275が画像入出力システム100のメモリカードI/F部270と接続された状態で制御が行われ、ユーザが操作部150に装備されているメモリカード内画像データキーを押下することにより、画像ファイルデータの復号・出力制御が開始される。制御装置110は、メモリカードI/F部270を介してメモリカード275に、画像入出力システム100にて出力するデータが蓄積されているかどうかを確認する(ステップS1301)。

【0088】例えばメモリカード275内には、図13

22

のメモリマップに示すように、暗号化された画像ファイルデータ(pic1, pgp)、暗号化されていない画像ファイルデータ(pic2, jpg)、暗号化された共通鍵暗号方式秘密鍵(cmnkey, pgp)、そしてプロパティファイル(prop, txt)とが蓄積されており、それらのデータをメモリカードI/F部270を介して制御装置110に転送する(ステップS1302)。データが蓄積されていない場合は、この制御を終了する。

【0089】次に、制御装置110は転送された各データについて拡張子を判別することにより、暗号化されているかどうかを検証する(ステップS1303)。暗号化ファイルが存在しなければ、メモリカード275中には暗号化データが存在していないと判断し、復号化の処理を行わず、プロパティファイルに記述されたプリントジョブ情報に基づいて画像を出力する(ステップS1308)。図5はプリントジョブ情報の一例を示す説明図である。「pic1, jpg, A4, SS, 1P」は、画像(pic1, jpg)をA4用紙(A4)に片面印刷(SS)で1部(1P)印刷するというものである。

【0090】暗号化データが存在するならば、そのデータを復号化するための「公開鍵暗号方式の秘密鍵」が画像入出力システム100に存在するかを確認し(ステップS1304)、該秘密鍵が存在しなければ、操作部150に「公開鍵暗号方式秘密鍵が存在しない」というメッセージを表示させる。このときユーザは、該当する公開鍵暗号方式秘密鍵をシステムに格納させる必要がある(ステップS1306)。

【0091】公開鍵暗号方式秘密鍵がシステムに存在するならば、それを用いて暗号化された共通鍵暗号方式秘密鍵を復号化する(ステップS1306)。そして、共通鍵暗号方式秘密鍵を用いて、暗号化された画像ファイルデータを復号化する(ステップS1307)。プロパティファイルが暗号化されていたら、公開鍵暗号方式秘密鍵で復号化し、そのプロパティファイルに記述されたプリントジョブ情報に基づいて画像出力処理を行う(ステップS1308)。

【0092】以上説明したように、本発明の第2の実施の形態に係る画像入出力システムによれば、制御装置110は、画像ファイルデータをメモリカード275に保存する際、画像ファイルデータを共通鍵暗号方式の秘密鍵を用いて暗号化し、共通鍵暗号方式の秘密鍵を公開鍵暗号方式の公開鍵を用いて暗号化し、暗号化された共通鍵暗号方式の秘密鍵と画像ファイルデータをメモリカード275に保存し、共通鍵暗号方式の秘密鍵を用いて暗号化され且つ共通鍵暗号方式の秘密鍵が公開鍵暗号方式の公開鍵を用いて暗号化され、メモリカード275に保存されている画像データを読み出して出力する際、上記暗号化された共通鍵暗号方式の秘密鍵を公開鍵暗号方式の公開鍵と対となる公開鍵暗号方式の秘密鍵で復号化

(13)

23

し、画像ファイルデータを上記復号化された共通鍵暗号方式の秘密鍵を用いて復号化し、出力する制御を行うと共に、復号化の際に拡張子に基づき暗号化データを判別する制御を行うため、下記のような効果を奏する。

【0093】データ量が大きいデータを暗号化する際、公開鍵暗号方式で暗号化するよりも共通鍵暗号方式で暗号化の方が時間を短縮させることができることを利用して、共通鍵暗号方式秘密鍵で暗号化し、その際用いた共通鍵暗号方式秘密鍵を公開鍵暗号方式公開鍵で暗号化することで、上記データが第三者によって改ざんされたり不正利用されたりすることを防止でき、データの信頼性を向上させることができるという効果を奏する。

【0094】また、メモ리카ード27に保存されたデータを画像出力システムにて出力する際、共通鍵暗号方式秘密鍵で暗号化されたデータ量の大きいデータを復号させるために用いる公開鍵暗号方式公開鍵で暗号化された共通鍵暗号方式秘密鍵を、公開鍵暗号方式秘密鍵で復号化し、上記データを上記復号化された共通鍵暗号方式秘密鍵で復号することで、出力する上記データの信頼性を向上させることができるという効果を奏する。

【0095】また、暗号化されたデータを復号化する際、暗号化されたデータと暗号化されていないデータとを判別することで、ユーザはより容易にデータの復号化を行うことが可能となる効果を奏する。

【0096】〔他の実施の形態〕上述した本発明の第1～第2の実施の形態においては、リーダ部及びプリンタ部を一体化した場合を例に上げたが、本発明はこれに限定されるものではなく、リーダ部及びプリンタ部を別構成とした場合、即ち、画像読取装置（リーダ装置）と画像形成装置（プリンタ装置）とを電気的に接続した場合にも適用可能である。

【0097】尚、本発明は、複数の機器から構成されるシステムに適用しても、1つの機器からなる装置に適用してもよい。上述した実施形態の機能を実現するソフトウェアのプログラムコードを記憶した記憶媒体を、システム或いは装置に供給し、そのシステム或いは装置のコンピュータ（またはCPUやMPU）が記憶媒体等の媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。

【0098】この場合、記憶媒体等の媒体から読み出されたプログラムコード自体が上述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体等の媒体は本発明を構成することになる。プログラムコードを供給するための記憶媒体等の媒体としては、例えば、フロッピディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、CD-R、磁気テープ、不揮発性のメモ리카ード、ROM、或いはネットワークを介したダウンロードなどを用いることができる。

【0099】また、コンピュータが読み出したプログラ

特開2002-91744

24

ムコードを実行することにより、上述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているOSなどが実際の処理の一部または全部を行い、その処理によって上述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0100】更に、記憶媒体等の媒体から読出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によって上述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0101】

【発明の効果】以上説明したように、請求項1～5記載の画像入力装置、請求項10～14記載の画像入出力装置、請求項19～23記載の画像データ暗号化方法、請求項28～31記載の記憶媒体によれば、画像データをメモ리카ードに保存する際、公開鍵暗号方式の公開鍵もしくは共通鍵暗号方式の秘密鍵を用いて暗号化することにより、画像データが第三者によって改ざんされたり不正利用されたりすることを防止でき、画像データの信頼性を向上させることができるという効果を奏する。

【0102】また、メモ리카ードに保存された画像データを画像出力装置にて出力する際、公開鍵暗号方式公開鍵で暗号化された画像データを公開鍵暗号方式秘密鍵で復号化することで、出力する画像データの信頼性を向上させることができるという効果を奏する。

【0103】請求項6～8記載の画像出力装置、請求項15～17記載の画像入出力装置、請求項24～26記載の画像データ復号化方法、請求項33～35記載の記憶媒体によれば、データ量が多い画像データを暗号化する際、公開鍵暗号方式で暗号化するよりも共通鍵暗号方式で暗号化の方が時間を短縮させることができることを利用して、共通鍵暗号方式秘密鍵で暗号化し、その際用いた共通鍵暗号方式秘密鍵を公開鍵暗号方式公開鍵で暗号化することで、画像データが第三者によって改ざんされたり不正利用されたりすることを防止でき、画像データの信頼性を向上させることができるという効果を奏する。

【0104】また、メモ리카ードに保存された画像データを画像出力装置にて出力する際、共通鍵暗号方式秘密鍵で暗号化されたデータ量の大きい画像データを復号させるために用いる公開鍵暗号方式公開鍵で暗号化された共通鍵暗号方式秘密鍵を、公開鍵暗号方式秘密鍵で復号化し、画像データを前記復号化された共通鍵暗号方式秘密鍵で復号することで、出力する画像データの信頼性を向上させることができるという効果を奏する。

【0105】請求項9記載の画像出力装置、請求項18

(14)

特開2002-91744

25

記載の画像入出力装置、請求項27記載の画像データ復号化方法、請求項36記載の記憶媒体によれば、暗号化された画像データを復号化する際、暗号化された画像データと暗号化されていない画像データとを判別することで、ユーザはより容易に画像データの復号化を行うことが可能となる効果を奏する。

【図面の簡単な説明】

【図1】本発明の第1及び第2の実施の形態に係る画像入出力システムの全体構成を示すブロック図である。

【図2】本発明の第1及び第2の実施の形態に係る画像入出力システムの内部構造を示す構成図である。

【図3】本発明の第1の実施の形態に係る公開鍵暗号方式を示す説明図である。

【図4】本発明の第1の実施の形態に係るメモリカードのメモリマップの一例を示す説明図である。

【図5】本発明の第1及び第2の実施の形態に係るプロパティファイルスクリプトの内容の一例を示す説明図である。

【図6】本発明の第1及び第2の実施の形態に係る画像入出力システムの操作部の一例を示す説明図である。

【図7】本発明の第1及び第2の実施の形態に係る画像入出力システムの操作部の一例を示す説明図である。

【図8】本発明の第1及び第2の実施の形態に係る画像入出力システムの操作部の一例を示す説明図である。

【図9】本発明の第1の実施の形態に係る画像入出力システムの動作を示すフローチャートである。

【図10】本発明の第1の実施の形態に係る画像入出力システムの動作を示すフローチャートである。

【図11】本発明の第1の実施の形態に係る画像入出力*

26

* システムの動作を示すフローチャートである。

【図12】本発明の第2の実施の形態に係る公開鍵暗号方式を示す説明図である。

【図13】本発明の第2の実施の形態に係るメモリカードのメモリマップの一例を示す説明図である。

【図14】本発明の第2の実施の形態に係る画像入出力システムの動作を示すフローチャートである。

【図15】本発明の第2の実施の形態に係る画像入出力システムの動作を示すフローチャートである。

【図16】本発明の第2の実施の形態に係る画像入出力システムの動作を示すフローチャートである。

【図17】本発明の画像データ暗号化方法、画像データ復号化方法を実行するプログラム及び関連データを記憶した記憶媒体の記憶内容の構成例を示す説明図である。

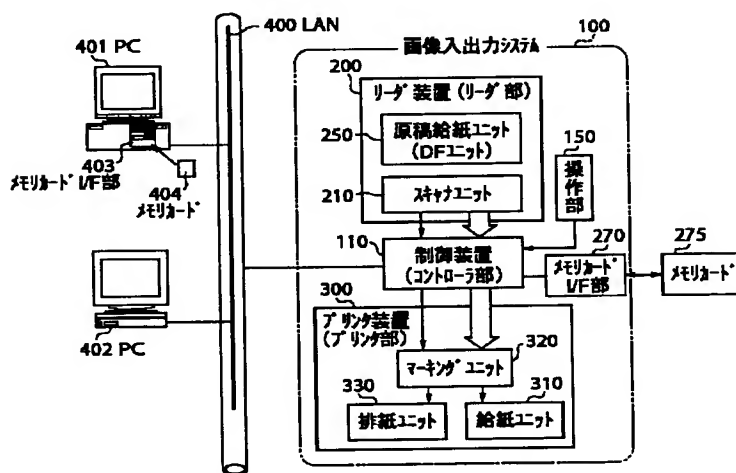
【図18】本発明の画像データ暗号化方法、画像データ復号化方法を実行するプログラム及び関連データが記憶媒体から装置に供給される概念例を示す説明図である。

【図19】共通鍵暗号方式と公開鍵暗号方式を示す説明図である。

【符号の説明】

100 画像入出力システム
110 制御装置
200 リーダ部
270 メモリカード I/F 部
275 メモリカード
300 プリンタ部
400 ネットワーク
401、402 PC

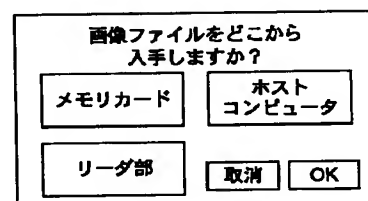
【図1】



【図5】

plc1.jpg,A4,SS,1P

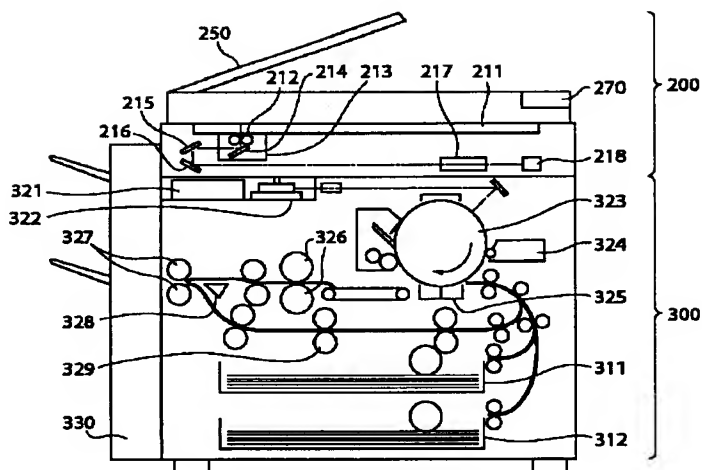
【図6】



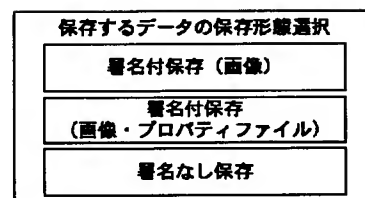
(15)

特開2002-91744

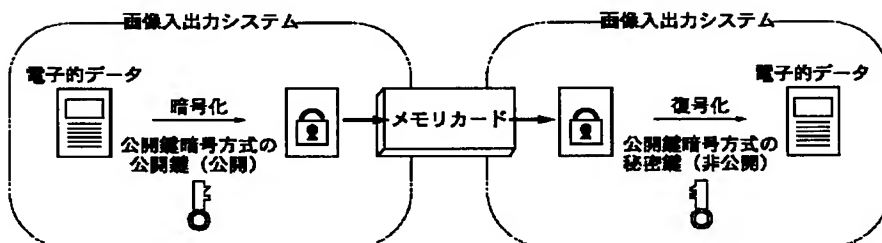
【図2】



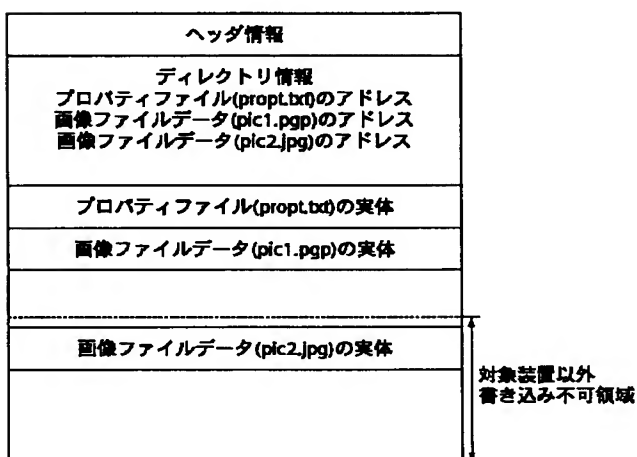
【図7】



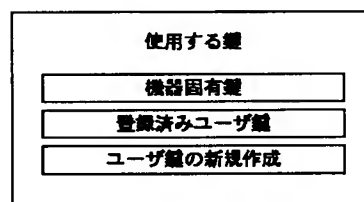
【図3】



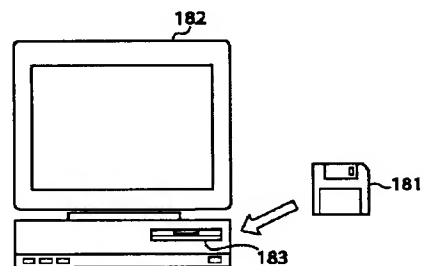
【図4】



【図8】



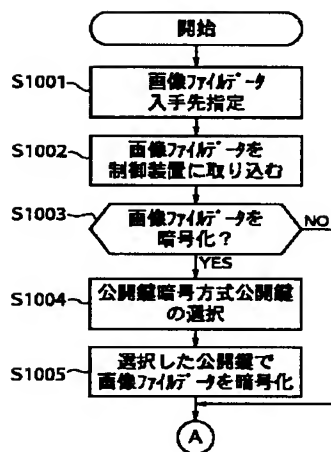
【図18】



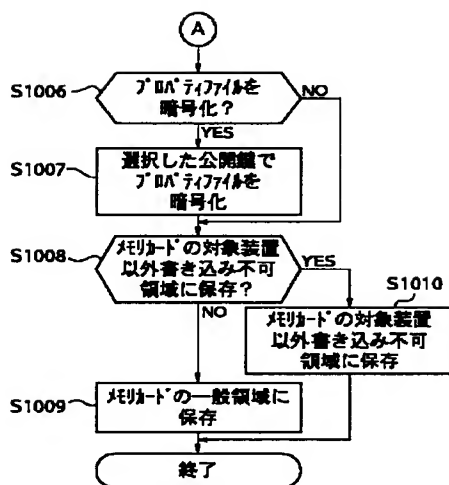
(16)

特開2002-91744

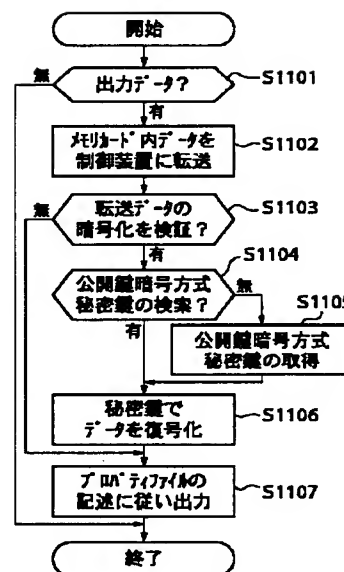
【図9】



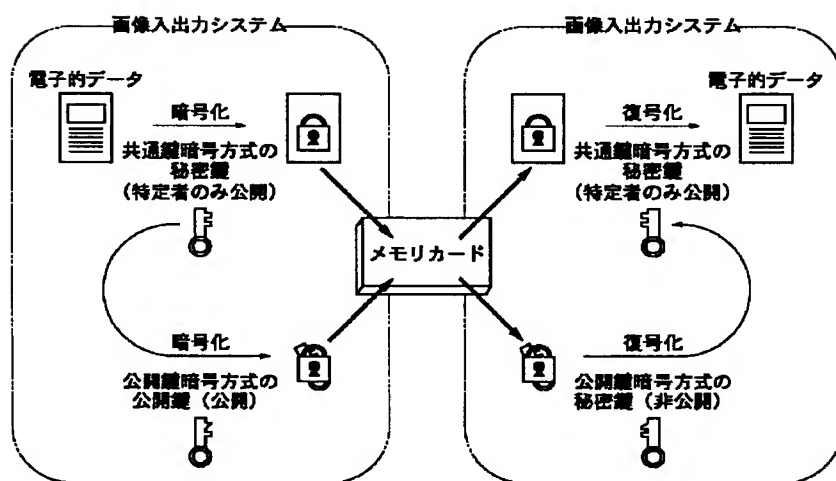
【図10】



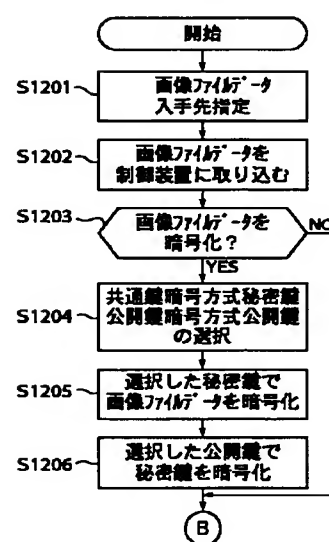
【図11】



【図12】



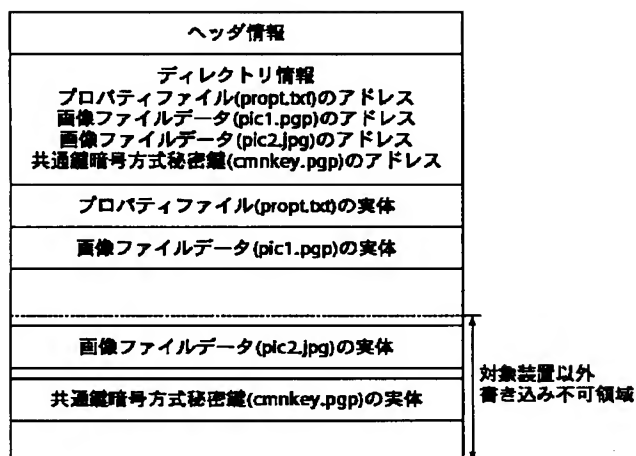
【図14】



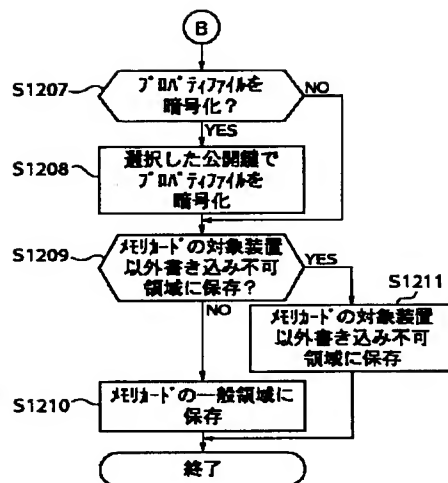
(17)

特開2002-91744

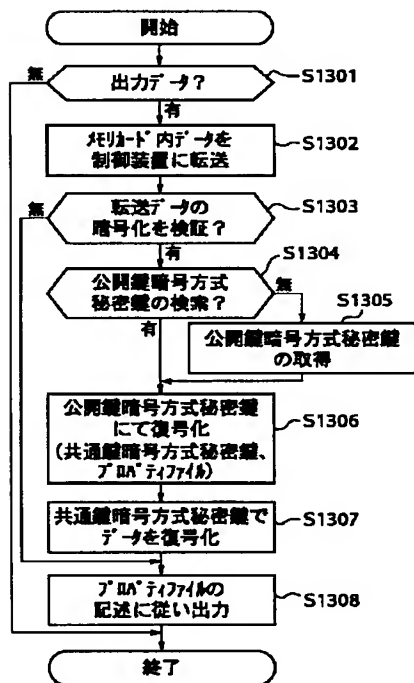
【図13】



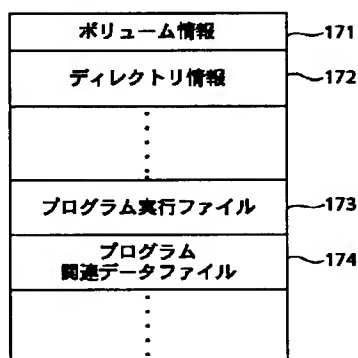
【図15】



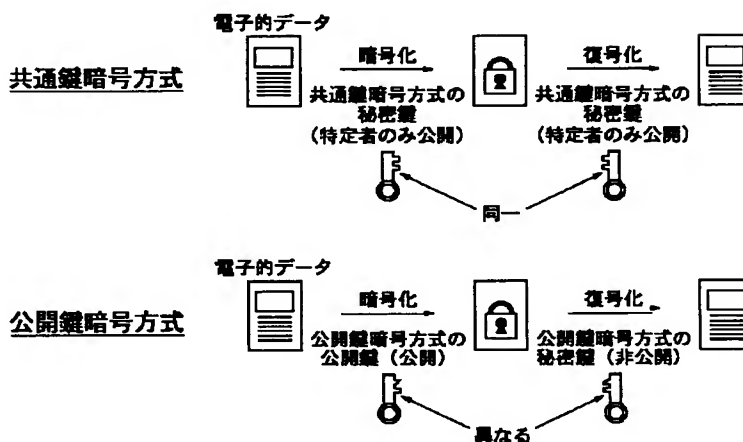
【図16】



【図17】



【図19】



(18)

特開2002-91744

フロントページの続き

(51)Int.Cl. ⁷	識別記号	F I	タームコード (参考)
G 0 9 C 1/00	6 4 0	B 4 1 J 29/00	Z
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 A
			6 0 1 C
			6 0 1 E

F ターム (参考) 2C061 AP01 AQ06 CL08 CL10
 2C087 AB05 BB10 BC12 BD53
 5B021 AA01 EE01 NN18
 5B058 CA27 KA02 KA04 KA06 KA08
 KA35
 5J104 AA01 AA09 AA12 AA16 EA06
 EA19 JA03 LA03 LA06 NA03
 NA35